We claim:

1. A method to detect fraudulent activities at a network-based transaction facility, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

2. A method as in claim 1 comprising causing the second identifier to be stored on the machine in responsive to the second event.

3. A method as in claim 2 comprising causing the lack of correspondence between the first identifier and second identifier to be detected at the machine.

4. A method as in claim 3 comprising receiving both the first identifier and the second identifier at the network-based transaction facility from the machine, and detecting the lack of correspondence between the first identifier and second identifier at the network-based transaction facility.

5. A method as in claim 4 comprising recording of the potentially fraudulent activity at the network-based transaction facility responsive to a detection of the lack of correspondence between the first identifier and the second identifier.

6. A method as in claim 5 wherein the second event is a transaction event, the method further comprising prohibiting a completion of the transaction event responsive to the detection of the lack of correspondence between the first identifier and the second identifier.

7. A method as in claim 6 comprising causing the first identifier to be stored on the machine within a cookie.

8. A method as in claim 7 comprising causing the first identifier and the second identifier to be recorded within the cookie.

9. A method as in claim 8 wherein the first event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility.

10. A method as in claim 9 wherein the transaction event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback

regarding a transaction, and updating a profile maintained by the network-based transaction facility.

11. A method as in claim 10 comprising:

causing the first identifier and the second identifier to be stored on the machine within a shill cookie;

causing a cookie identifier to be stored within the shill cookie;

causing the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine;

causing the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the second transaction event with the network-based transaction facility using the machine;

causing the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility;

causing the cookie bundle to be inspected for the potentially fraudulent activity; and

causing the potentially fraudulent activity to be recorded into a database.

12. A method as in claim 11 wherein an inspection of the shill cookie comprises a source for the detection of the lack of correspondence between the first identifier and the second identifier.

13. A method as in claim 12 further comprising:

causing the cookie bundle to be a non-session cookie residing on the machine for a predetermined amount of time.

14. A method as in claim 13 further comprising:

causing the shill cookie to be appended every time a new user identifier is used to establish a new event with the network-based transaction facility using the machine wherein there is a lack of correspondence between the new user identifier and the first user identifier.

15. A method as in claim 14 wherein the machine comprises a computer connected to the network-based transaction facility.

16. A method as in claim 15 wherein the network-based transaction facility comprises an Internet-based auction facility.

17. A method as in claim 16 further comprising:

causing the shill cookie to record and to store a predetermined number of user identifiers.

18. A method as in claim 17 further comprising causing the shill cookie and the cookie bundle to be encoded such that the shill cookie and the bundle cookie are coded.

19. A method as in claim 18 further comprising causing the shill cookie and the cookie bundle to be encrypted.

20. A method as in claim 19 further comprising:

generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;

recording each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table;

updating the potential fraudulent activities table at least on a periodic basis; and

providing an updated report of the potential fraudulent activities table to an investigation team.

21. A method as in claim 20 further comprising:

configuring the potential fraudulent activities table to include a transaction product category field, a transaction country field, a transaction price range field, and a transaction activity field.

22. A method as in claim 21 wherein the new event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility.

23. A method as in claim 22 further comprising providing the updated report to the investigation team at a predetermined time.

24. A method as in claim 23 further comprising providing the network-based transaction facility with a capability to override the updated report to the investigation team as necessary.

25. A method as in claim 24 further comprising providing a priority ranking system having a low priority for a low potential fraudulent activity frequency, a medium priority for a medium potential fraudulent activity frequency and a high priority for a high potential fraudulent activity frequency.

26. A method as in claim 25 further comprising examining the updated report to confirm the potentially fraudulent activity.

27. A method as in claim 26 wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks.

28. A method as in claim 27 wherein the recording does not affect any one of the first event, the second event, and the new event.

29. A method as in claim 28 further comprising causing the detection of the potentially fraudulent activity responsive a matching of at least two user transaction preferences from at least two different user identifies.

30. A method as in claim 29 wherein the user transaction preferences comprise credit card numbers, bidding histories, payment methods, and shipping addresses.

31. A computer readable medium comprising instructions, which when executed on a processor, cause the processor to perform a method for detecting suspicious transactions made over a network-based transaction facility using a client machine, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

32. A method for detecting suspicious transactions made with an Internet service facility from one computerized facility, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine, the causing being responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity, the detecting being responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

33. A system to detect fraudulent activities at a network-based transaction facility, the system comprising:

an identifier process to cause a first identifier associated with a first user identity to be stored on a machine responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

a first detection process to detect a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

34. A system as in claim 33 comprising a second detection process to cause the lack of correspondence between the first identifier and second identifier to be detected at the machine.

35. A system as in claim 34 wherein said second detection process includes receiving both the first identifier and the second identifier at the network-based transaction facility from the machine, and detecting the lack of correspondence between the first identifier and second identifier at the network-based transaction facility.

36. A system as in claim 35 comprising a first recording process to record the potentially fraudulent activity at the network-based transaction facility responsive to a detection of the lack of correspondence between the first identifier and the second identifier.

37. A system as in claim 36 comprising a cookie recording process to record the first identifier and the second identifier to be recorded within a cookie.

38. A system as in claim 37 comprising:

a storing process to cause the first identifier and the second identifier to be stored on the machine within a shill cookie and a cookie identifier to be stored within the shill cookie;

a bundling process to cause the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine;

a sending process to cause the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the

second transaction event with the network-based transaction facility using the machine;

an appending process to cause the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility;

an inspection process to cause the cookie bundle to be inspected for the potentially fraudulent activity; and

a second recording process to cause the potentially fraudulent activity to be recorded into a database.

39. A system as in claim 38 further comprising:

a tabulating process to generate a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;

a third recording process to record each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table;

an updating process to update the potential fraudulent activities table at least on a periodic basis and to provide an updated report of the potential fraudulent activities table to an investigation team.

40. A system to detect fraudulent activities at a network-based transaction facility, the system comprising:

a first means for causing a first identifier associated with a first user identity to be stored on a machine responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

a second means for detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine.